OSINT-ТЕХНОЛОГИИ В ЗАДАЧАХ ВЫЯВЛЕНИЯ ПОВЕРХНОСТИ АТАК КОРПОРАТИВНЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Лапина С.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Насонова Н.В. – д-р техн. наук, доцент

Аннотация. Рассматривается применение OSINT-технологий для выявления внешней поверхности атак корпоративных инфокоммуникационных систем. Сформулирована гипотеза о том, что использование OSINT при инвентаризации и верификации ресурсов позволяет точнее выявлять внешние точки входа и сопоставлять их с архитектурой сети организации. Предложена трёхэтапная методика исследования, включающая сбор открытых сведений о ресурсах, формирование карты поверхности атак и её сопоставление с сегментами корпоративной сети. На примере компании показана практическая ценность подхода для специалистов по информационной безопасности, мониторинга и подготовки данных для классификации систем.

Ключевые слова. OSINT, корпоративная инфокоммуникационная система, VPN, DMZ, SOC.

Современные корпоративные инфокоммуникационные системы изменяются быстрее, чем внутренние реестры ресурсов и эксплуатационная документация. Организации публикуют веб-сервисы, тестовые стенды, каналы удалённого доступа и облачные интеграции, однако эти изменения не всегда своевременно отражаются во внутреннем учёте. В результате возникает разрыв между тем, как система описана внутри организации, и тем, как она выглядит для внешнего наблюдателя. Для специалистов по информационной безопасности это критично, поскольку атакующий начинает именно с открытой разведки: изучает домены, поддомены, сертификаты, VPN-шлюзы, почтовую инфраструктуру и иные признаки публикации сервисов [1].

Поверхность атаки корпоративной инфокоммуникационной системы определяется как совокупность всех доступных для воздействия извне и из смежных контуров ресурсов, интерфейсов, сервисов, учётных записей, каналов связи и точек интеграции, через которые потенциально может быть реализована атака. Её выявление включает инвентаризацию ресурсов, анализ сетевой архитектуры и периметра, проверку внешней доступности узлов и сервисов, а также поиск потенциально уязвимых точек взаимодействия между локальными, удалёнными и облачными сегментами.

Применение OSINT-технологий, включающее накопление и анализ данных, полученных из открытых источников в интернете, в процессах инвентаризации и верификации ресурсов позволяет построить более полную и актуальную карту внешней поверхности организации, чем при опоре только на внутренние описания. При этом OSINT рассматривается не как единственный способ инвентаризации, а как средство её дополнения и проверки за счёт независимого анализа внешне наблюдаемых ресурсов.

Методика выявления и картирования внешней поверхности атаки корпоративной инфокоммуникационной системы с использованием OSINT (рисунок 1) представляет собой трёхэтапный процесс инвентаризации внешних ресурсов, их классификации по типам сервисов и сопоставления с архитектурой корпоративной сети для оценки потенциальных точек внешнего воздействия. На первом этапе собираются открытые сведения о внешних ресурсах: домены и поддомены, публичные IP-адреса, TLS-сертификаты, почтовые записи, точки VPN-доступа. Для этого могут использоваться Amass и theHarvester для поиска доменов и поддоменов, crt.sh и SecurityTrails для анализа DNS-, MX- и сертификатных данных, а также Shodan и Censys для выявления опубликованных сервисов и их сетевых признаков. На втором этапе ресурсы группируются по функциональным категориям: веб-доступ, почта, удалённый доступ, интеграционные сервисы. На третьем этапе результаты сопоставляются с архитектурной моделью корпоративной сети: определяется, в каком периметровом сегменте расположен внешний сервис, куда он должен передавать трафик, какие внутренние сегменты и средства мониторинга затрагиваются.

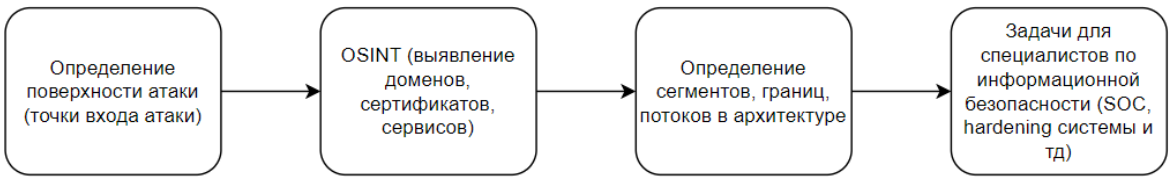

Рисунок 1 – Последовательность выявления поверхности атак с помощью OSINT в корпоративной инфокоммуникационной системе

На практике основной результат исследования состоит не в получении списка доменных имён, а в построении проверяемой модели внешнего периметра. Предложенная методика была апробирована на модели корпоративной инфокоммуникационной системы страховой компании. Для компании были выделены публичные веб-сервисы, почтовая инфраструктура и канал VPN-доступа. Каждая внешняя точка входа сопоставлялась с конкретным сетевым сегментом: клиентский портал относился к DMZ WEB, VPN-шлюз – к DMZ VPN, почтовый узел – к DMZ MAIL. Далее определялись допустимые потоки во внутренний контур: DMZ WEB – SERVER APP – DB LAN, DMZ VPN – SERVER APP и SERVER INFRA, а журналы всех периметровых компонентов направлялись в SEC LAN. Такое сопоставление позволило актуализировать контекстную схему корпоративной сети, выделить критичные границы доверия и уточнить перечень системных контуров, присутствующих в архитектуре [3].

Для повышения наглядности результаты целесообразно представлять не только в виде схемы, но и в виде компактной таблицы соответствий (таблица 1).

Таблица 1 – Сопоставление внешних ресурсов с архитектурной моделью корпоративной инфраструктуры

Внешний актив	Назначение	Сетевой сегмент	Внутренняя точка назначения
client-portal.company.by	Клиентский веб-доступ	DMZ WEB	SERVER APP
vpn.company.by	Удаленный доступ филиалов	DMZ VPN	SERVER APP / SERVER INFRA
mail.company.by	Почтовый обмен	DMZ MAIL	Mail system
api.company.by	Интеграционный сервис	DMZ WEB	SERVER APP

Построенная таблица показывает, что исследование с использованием OSINT может быть непосредственно преобразовано в инженерные артефакты для специалистов по информационной безопасности. Если внешний сервис существует, но не имеет места в архитектурной модели, это означает наличие неучтённого ресурса либо устаревшей документации. Если же ресурс отражён в схеме, но не имеет владельца, допустимого маршрута и источника логов, то организация получает зону повышенного риска, которую сложно контролировать и защищать.

На основе построенной карты внешней поверхности и уточнённой архитектурной модели были выделены ключевые системные контуры: веб-канал обслуживания, корпоративные сервисы, прикладные бизнес-сервисы и контур мониторинга. Для каждого контура определялись виды обрабатываемых данных, допустимые потоки и требования к мониторингу, что создаёт основу для последующего отнесения систем к классам типовых ИС по требованиям регулятора [2].

Таблица 2 – Выделение информационных систем по данным внешнего периметра и архитектурной модели

ИС	Ключевые данные	Размещение	Практический результат
ИС-1 Веб-канал	ПД клиентов, учетные записи	DMZ WEB, SERVER APP, DB LAN	Контроль публикации порталов и API
ИС-2 Корпоративная инфраструктура	Учетные записи, почта, файлы	SERVER INFRA, MGMT LAN	Уточнение состава сервисов удаленного доступа
ИС-3 Бизнес-логика	Договоры, обращения, вложения	SERVER APP, DB LAN, FILE SRV	Понимание критичных потоков к данным
ИС-4 Киберцентр	Логи, телеметрия, инциденты	SEC LAN, BACKUP LAN	Определение источников событий и мониторинга

Анализ результатов показывает, что OSINT целесообразно рассматривать как постоянный процесс подразделения информационной безопасности, а не как разовую исследовательскую процедуру. Его практическая ценность проявляется в трёх направлениях: выявление теневых и забытых ресурсов, проверка полноты архитектурной документации, повышение качества мониторинга в SOC. При этом OSINT не заменяет внутренний аудит и требует верификации со стороны владельцев систем, однако в качестве первичного средства контроля внешнего периметра позволяет быстрее обнаруживать расхождения между реальной внешней поверхностью корпоративной инфокоммуникационной системы и её формальным описанием.

Список использованных источников:

1. Makrushin, A. Attack Surface Analysis and Monitoring using Open-Source Intelligence / A. Makrushin. – 2022.

2. О внесении изменений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 : приказ ОАЦ от 30.12.2021 № 195.

3. Information security, cybersecurity and privacy protection – Information security controls : ISO/IEC 27002:2022.